WILLKIE FARR & GALLAGHER LLP
Benedict Y. Hur (SBN: 224018)
Simona Agnolucci (SBN: 246943)
Jayvan E. Mitchell (SBN: 322007)
Amanda Maya (SBN: 324092)
One Front Street, 34th Floor
San Francisco, CA 94111
Telephone: (415) 858-7400
Facsimile: (415) 858-7599
bhur@willkie.com
sagnolucci@willkie.com
jmitchell@willkie.com
amaya@willkie.com

Attorneys for
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO

ANIBAL RODRIQUEZ AND JULIE ANNA MUNIZ, individually and on behalf of all other similarly situate

Plaintiff

vs

GOOGLE LLC, *et al*.

Defendant.

Case No. 3:20-CV-04688

DEFENDANT GOOGLE LLC's MOTION TO DISMISS COMPLAINT PURSUANT TO FED. R. CIV. P. 12(B)(6)

The Honorable Richard Seeborg

Court: Courtroom 3 – 17th Floor
Date: December 17, 2020
Time: 1:30 p.m.

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

Please take notice that, on December 17, 2020, the undersigned will appear before the Honorable Richard Seeborg of the United States District Court for the Northern District of California at the San Francisco Courthouse, Courtroom 3, 17th Floor, 450 Golden Gate Avenue, San Francisco, CA 94102, and shall then and there present Defendant Google LLC's Motion to Dismiss (the "Motion").

The Motion is based on this Notice of Motion and Motion, the attached Memorandum of Points and Authorities, the accompanying Request for Judicial Notice and exhibits attached thereto, the pleadings and other papers on file in this action, any oral argument, and any other evidence that the Court may consider in hearing this Motion.

ISSUES PRESENTED

Whether Plaintiffs fail to state a claim upon which relief can be granted, thus warranting dismissal of the Complaint (Counts I–IV) under Fed. R. Civ. P. 12(b)(6).

RELIEF REQUESTED

Google requests that the Court dismiss the Complaint with prejudice.

DATED: October 13, 2020

Respectfully submitted,

WILLKIE FARR & GALLAGHER LLP

By: /s/ *Benedict Y. Hur*

Benedict Y. Hur

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes, Rules and Regulations

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiffs bring claims for alleged constitutional and statutory violations of privacy because certain third-party apps (such as Lyft) used a tool called Google Analytics for Firebase ("Firebase") to analyze the activities of their users in order to improve the app. Of course, as a condition of using Firebase, the apps authorized Google to collect their users' data. The apps also notified their users that they were using Firebase and obtained consent to the collection from their users. Accordingly, none of Plaintiffs' claims can survive.

Plaintiffs' theory hinges on a single allegation about an account-level setting called Web & App Activity ("WAA"). When WAA is "on," it allows Google to *save* a user's online searches and activity in the user's account to help Google provide faster, more relevant searches and other forms of personalized experiences across Google services. Plaintiffs allege that when they turned "off" the WAA setting--meaning Google would not save users' online search history in the users' Google accounts--that somehow meant that third-party apps could not separately authorize Firebase to collect and analyze information about users' activities on those apps. Neither the law nor common sense supports Plaintiffs' theory.

First, separate and apart from WAA, the apps and Plaintiffs consented to the collection. There can be no plausible Wiretap Act, CIPA, Invasion of Privacy or CDAFA claim when the Plaintiffs consented to the allegedly wrongful actions.

Second, the Wiretap Act claim fails even if Plaintiffs had not consented to Google's collection, because it requires only consent from one party, which the apps provided by using Firebase to collect their users' data.

Third, the California Invasion of Privacy Act and California Constitutional claims both fail, not only because of user consent, but because the actions alleged here cannot plausibly plead a privacy violation. Courts in this district have made it clear that even if Plaintiffs had not consented, the collection of the basic and anonymized Internet data at issue here does not constitute an egregious breach of social norms.

Finally, Plaintiffs' CDAFA claim is frivolous. Even if Plaintiffs could allege lack of consent by the apps (they cannot), Plaintiffs allege that Google violated the CDAFA by collecting data from apps using software (Firebase) that app developers intentionally integrated into their apps for that very purpose. But CDAFA requires that a defendant access data by circumventing technical or code-based barriers put in place to restrict access to the information. Plaintiffs' allegations cannot plausibly support a CDAFA claim.

The Court should dismiss the Complaint with prejudice for failure to state a claim under Rule 12(b)(6).

II. BACKGROUND AND PLAINTIFFS' ALLEGATIONS

A. Developers Voluntarily Integrated Firebase Into their Apps.

Google LLC ("Google") is a technology company that offers popular products, including analytics software and services for websites and apps. Compl. ¶¶ 14, 22, 32. Firebase Software Development Kit ("Firebase SDK") is a Google product that developers integrate into their apps in order to access Google analytics services and added app functionality, among other things. *See id.* ¶¶ 8, 29, 33, 40. "At the heart of Firebase is Google Analytics, a free and unlimited analytics solution." *See also* Compl. ¶ 41, n.8. App developers use Google Analytics for Firebase as a tool to collect their users' app usage data so they can improve their experiences. *Id.* As used herein, "Firebase" refers to Google Analytics for Firebase, while "Firebase SDK" refers to the Firebase development platform as a whole.

If used by the app, Firebase automatically captures certain data every time a user interacts with the apps: (i) the title of the page that users viewed in the apps, (ii) the "page_referrer" (i.e., if the user arrived at that page via another page), and (iii) the page URL. *Id.* ¶ 38. Plaintiffs allege that this data reveals user device information, including "unique identifying information to the device" (*id*. ¶ 57), but do not allege that Firebase collects any personally identifiable information that connects the user to the data. Plaintiffs also variously allege that Firebase collects "personal information and communications" (*id*. ¶ 59), "private personal information consumers wish and expect to protect" (*id*. ¶ 60), and "detailed URL requests, app browsing histories, and search queries

which Plaintiffs sent to those apps" (*id.* ¶ 116). However, these allegations are wholly conclusory and Plaintiffs do not specifically allege what data was collected, how such data is collected, what information was included therein, or why it is "private personal information."

B. The Apps Consented to Google's Collection of Plaintiffs' Data.

Plaintiffs are individuals who allegedly used the Lyft, Alibaba, and Shazam apps on their Android and Apple smartphones in 2019 and 2020. *Id.* ¶¶ 93–98. Plaintiffs allege that these apps chose to use Firebase as a tool and that Google thereby collected Plaintiffs' app activity data without their consent. By without consent, Plaintiffs mean that Google collected that data while WAA was turned off in Plaintiffs' Google Accounts settings. *See id.* ¶¶ 99. But WAA is an account-level setting that allows Google to save users' activity in their respective Google Accounts when turned "on," and has nothing to do with what data Firebase collects. *See infra* § E. Plaintiffs also fail to mention that both the apps and Plaintiffs themselves consented to Google receiving the data, as evidenced by the agreements between Google and the apps and between the apps and users.

Developers integrate Firebase into their apps to analyze how their customers use the app, which they do by authorizing Firebase to collect users' app activity data. The Firebase Terms of Service agreement ("Firebase ToS") defines Firebase as "the Firebase Software Development Kit, which *is used or incorporated in an App for the purpose of collecting Customer Data*, together with any fixes, updates and upgrades provided to You." Defendant's Request for Judicial Notice ("RJN"), ¶ 1; Declaration of Andrew Rope ("Rope Decl.") ¶ 2 and Ex. 1(a)–(b), pp. 2, 12 (emphasis added). The Google Analytics for Firebase Use Policy ("Firebase Use Policy") also makes clear that by subscribing to Google's Firebase service, app developers authorize Google to collect their users' app activity data. The Firebase Use Policy states, in relevant part, that: "[b]y enabling Google Analytics for Firebase you enable the collection of data about App Users, including via identifiers for mobile devices (including Android Advertising ID and Advertising Identifier for iOS), cookies and similar technologies." Rope Decl. ¶ 3 and Ex. 2(a)–(b), pp. 1, 3; RJN ¶ 2.

C. Google Required the Apps to Disclose the Use of Firebase to Collect Users' Data and to Get Users' Consent.

The Firebase ToS requires the apps to (1) disclose their use of Firebase to users, and (2) obtain their users' consent to the storing and accessing of their Data by Google:

> You must post a Privacy Policy and that Privacy Policy must provide notice of Your use of cookies, identifiers for mobile devices (e.g., Android Advertising Identifier or Advertising Identifier for iOS) or similar technology that are used to collect data. You must disclose the use of the [Firebase] Service, and how it collects and processes data. . . .You will use commercially reasonable efforts to ensure that a User is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information on the User's device where such activity occurs in connection with the Service and where providing such information and obtaining such consent is required by law.

Rope Decl. ¶ 2 and Ex. 1(a)–(b), pp. 5, 14. Consistent with this requirement, each of the apps Plaintiffs identify in the Complaint disclosed that they use Firebase to collect user Data.[1] Alibaba's Privacy Policy explicitly states that:

> Our Platform uses Google Analytics, an internet analytics service provided by Google, Inc. ("Google"). Google's cookies allow us to analyze use of the Platform by telling us which pages our users are viewing, which ones are most popular, what time of day our Platform are visited, if users have previously visited our Platform, from which website users are redirected to our Platform were and the like. The data generated by the cookie about your use of the Platform will be transmitted to Google and stored by Google on servers in the United States.

Declaration of Jayvan E. Mitchell ("Mitchell Decl.") ¶ 3 and Ex. B(1)-(4); RJN ¶ 4. Lyft's Privacy Policy similarly states that "[w]e collect information through the use of 'cookies,' tracking pixels, data analytics tools like Google Analytics, SDKS, and other third party technologies to understand how you navigate through the Lyft Platform and interact with Lyft advertisements…." Mitchell Decl. ¶ 5 and Ex. D(1)–(3), pp. 3, 16; *see also id.* at pp. 30; RJN ¶ 6. The Shazam app for iOS devices, from which Plaintiff Muniz alleges Google collected her app activity data in 2020 (Compl. ¶ 95), does not have such a disclosure because it did not use Firebase in 2020 (Mitchell Decl. ¶ 6

[1] Plaintiff JulieAnn Muniz alleges that Google collected her App use data from the Shazam and Lyft apps, which she used on her Apple device at various times in 2020. Compl. ¶¶ 93–95. Plaintiff Anibal Rodriquez alleges that Google collected his App use data from the Lyft and Alibaba apps on his Android device in 2019 and 2020. Compl. 96–98.

and Ex. E; RJN ¶ 7).

Alibaba's and Lyft's privacy policies are both incorporated into their respective terms of service agreements, which users must agree to as a condition of using the apps. Alibaba's Terms of Use agreement states in the preamble that: "[b]y accessing and using the Sites and Services, you agree to accept and be bound by the Terms" Mitchell Decl. ¶ 2 and Ex. A(1)–(7), pp. 1, 19, 40; *see also id.* at pp. 55, 71, 88, 104; RJN ¶ 3. Lyft's Terms of Use agreement similarly provides that: "[i]f you do not agree to be bound by the terms and conditions of this agreement, you may not use or access the Lyft platform for any of the services provided through the Lyft platform." Mitchell Decl. ¶ 4 and Ex. C(1)-(3), pp. 1, 38, 80–81; RJN ¶ 5. Thus, in addition to the apps authorizing Google's access to users' app activity data, the users themselves (including Plaintiffs) also consented.

D. The Firebase Terms of Service and Use Policy Forbid the Apps from Sending Personally Identifiable Information to Google.

Plaintiffs do not allege that the data Google received was personally identifiable. This is not surprising given that the Firebase ToS forbids apps from sharing users' personally identifiable information with Google. The Firebase ToS provides that apps "will not, and will not assist or permit any third party to, pass information to Google that Google could use or recognize as personally identifiable information." Rope Decl. ¶ 2 and Ex. 1(a)–(b), pp. 4, 14. The Firebase Use Policy similarly mandates that apps "will not facilitate the merging of personally-identifiable information with non-personally identifiable information unless you have robust notice of, and the user's prior affirmative (i.e., opt-in) consent to, that merger." *Id.* ¶ 3 and Ex. 2(a)–(b), pp. 1, 3.

E. Google's Disclosures Do Not Suggest that Turning Off WAA Prevents Google from Receiving Data from Apps.

Plaintiffs allege that Google led them to believe that Google would "stop collecting all of their mobile app information or activity" if WAA was turned off. Compl. ¶ 51. Plaintiffs' expectation was purportedly based on language excerpted from various disclosures by Google and quoted in the Complaint. *See id.* ¶¶ 50, 52. But this language and the source documents do not plausibly support Plaintiffs' purported expectation.

For example, Plaintiffs patch together language from a Google Help Center web page titled "See & Control your Web & App Activity," that supposedly "describes how Google collects detailed user information when Web & App Activity is on." *Id.* ¶ 50. As told by Plaintiffs, this language suggests that Google would "stop collecting *all* of their mobile app information or activity if the 'Web & App Activity' setting is turned 'off.'" *Id.* ¶ 51. But no reasonable person would interpret that language to mean that Google stops receiving *all* data when WAA is turned off. The webpage states that: "[i]f Web & App Activity is turned on, your searches and activity from other Google services are ***saved in your Google Account***, so you may get more personalized experiences, like faster searches and more helpful app and content recommendations." *See id.* ¶ 49, n.11 (emphasis added). Contrary to Plaintiffs' allegation, this web page merely informs users what to do if they do not want their Web & App Activity to be saved in their Google Account. It is not reasonable or plausible for Plaintiffs to infer that, by informing users that Google will not save certain browsing data in their Google Accounts when WAA is off, Google stopped receiving all data those users sent. And it certainly does not suggest that turning off WAA prevents Google from collecting the data that apps and users separately authorized Google to receive.

III. LEGAL STANDARD

A complaint must be dismissed where the plaintiff fails to allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). In determining if a plaintiff has stated a claim, a court accepts as true only well-pleaded factual allegations in the complaint. *See Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009). A court begins its analysis of a complaint by "identifying pleadings that, because they are no more than conclusions, are not entitled to the presumption of truth." *Id.* The court also "need not. . .accept as true allegations that contradict matters properly subject to judicial notice," or that are "unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Secs. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (citation omitted). Taking only "well-pleaded factual allegations" as true, a court then "determine[s] whether they plausibly give rise to an entitlement to relief." *Iqbal*, 556 U.S. at 679. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the

reasonable inference that the defendant is liable for the misconduct alleged." *Id*. at 678. This standard "asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.*

Here, Plaintiffs' Complaint fails to state a claim and should be dismissed on all counts pursuant to Rule 12(b)(6).

IV. ARGUMENT

Plaintiffs have not alleged any facts that plausibly establish that they are entitled to relief under any of the four causes of actions alleged in the Complaint. Plaintiffs' claims all fail because Plaintiffs consented to the collection of their app activity data after Google obtained consent from the apps. The claims also fail because: (i) Google's collection was authorized by both Plaintiffs and the apps and is thus exempt under the Wiretap Act (Count I), (ii) Plaintiffs fail to sufficiently plead what data was collected never mind how, under the circumstances, they had a reasonable expectation of privacy in that data (Counts II and III), (iii) Plaintiffs fail to plead that collection of the app activity data was highly offensive (Count III), and (iv) Plaintiffs do not allege that Google circumvented any technical or code-based barriers in order to access their app activity data (Count IV).

A. Each Claim Fails Because Google was Authorized to Receive Plaintiffs' Data (All Counts).

All of Plaintiffs' claims hinge on the contention that because Plaintiffs turned off the WAA setting, Google could not collect basic Internet traffic data the Plaintiffs voluntarily provided to certain apps. *See, e.g.,* Compl. ¶¶ 121, 131, 140, 152. Plaintiffs' premise is faulty because WAA collects different data in a different way than Firebase, and because turning off WAA means only that data will not be stored in a user's Google Account. Each claim fails because the Plaintiffs consented to the apps' use of Firebase to collect the data that users provided. Because user consent is fatal to each claim, the Complaint should be dismissed without leave to amend. *See, e.g., In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1026 (N.D. Cal. 2014) ("Since the Wiretap Act concerns the *unauthorized* interception of electronic communication, the consent of one party is a complete defense to a Wiretap Act claim.") (Count I); *In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d

589, 607 (9th Cir. 2020) (citing Cal. Pen. Code § 631(a) ("CIPA prohibits any person from using electronic means to 'learn the contents or meaning' of any 'communication' 'without consent' or in an 'unauthorized manner.'") (Count II); *Diaz v. Messer*, 742 F. App'x 250, 252 (9th Cir. 2018) ("Section 632(a) prohibits recording a 'confidential communication' without the consent of all parties involved.") (Count II); *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016) (noting that consent means a plaintiff cannot have a reasonable expectation of privacy under the California Constitution) (Count III); *Oracle USA, Inc. v. Rimini Street, Inc.*, 879 F.3d 948, 962 (9th Cir. 2018) (plaintiffs cannot state a claim under CDAFA where the defendant had authorization to take and use the information at issue) (Count IV).

1. The apps used Firebase as a tool to collect their users' data and affirmatively authorized Google's collection.

Plaintiffs allege that app developers intentionally integrated Firebase into their apps, fully aware that Firebase automatically collects users' app activity data. *See* Compl. ¶ 33 ("Google itself explains to app developers that "Firebase's '[a]utomatically collected events are triggered by basic interactions with your app. As long as you use the Firebase SDK, you don't need to write any additional code to collect these events."). The Firebase ToS makes clear that app developers integrate Firebase into their apps in order to collect user's app activity data. For example, Firebase is defined in the ToS as "the Firebase Software Development Kit, which *is used or incorporated in an App for the purpose of collecting Customer Data*, together with any fixes, updates and *upgrades* provided You." *See supra* § II(B) (emphasis added). The Firebase Use Policy also makes clear that by subscribing to Google's Firebase service, app developers authorize Google to collect and use their users' app activity data: "[b]y enabling Google Analytics for Firebase you enable the collection of data about App Users, including via identifiers for mobile devices (including Android Advertising ID and Advertising Identifier for iOS), cookies and similar technologies." *Id.*

2. Google requires the apps to disclose the use of Firebase to users and obtain their consent to data collection.

As discussed *supra* § II(C), Section 7 of the Firebase ToS, titled "Privacy," requires the apps to disclose their use of Firebase to collect users' data and get users' consent:

> You must disclose the use of the [Firebase SDK] Service, and how it collects and processes data .... You will use commercially reasonable efforts to ensure that a User is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information on the User's device where such activity occurs in connection with the Service and where providing such information and obtaining such consent is required by law.

Thus, as a condition of using Firebase to collect their users' information, the apps agreed to obtain consent to the collection. As explained below, the apps Plaintiffs have identified obtained the required consent.

3. The apps both disclose their use of Firebase and require users to agree to the collection of their data.

Consistent with the Firebase ToS, each of the apps identified in the Complaint disclosed to users that their app activity data was being collected using Google' Firebase service.[2] As discussed supra § II(C), Alibaba's Privacy Policy discloses that Alibaba uses Google Analytics for Firebase, and that data regarding users' page views and visiting history is transmitted to, and stored by, Google. Lyft's Privacy Policy similarly discloses that Lyft collects information through data analytics tools like Google Analytics to understand users' navigation behavior and response to advertisements. *See supra* § II(C). Both Alibaba's and Lyft's privacy policies are incorporated into their terms of service agreements, which users must consent to in order to use the apps. Thus, in addition to the apps authorizing Google to access users' data, the users themselves (including Plaintiffs) also consented. Because Plaintiffs consented to the collection of the data that forms the basis of each claim, the Complaint should be dismissed in its entirety with prejudice.

[2] As explained *supra* § II(C), the Shazam app for Apple did not use Firebase in 2020 and Google therefore could not have used Firebase to collect Plaintiff Muniz's Data from Shazam on her Apple device in 2020, as Plaintiffs allege. Complaint ¶ 95.

B. Plaintiffs Fail to State a Claim Under the Federal Wiretap Act because the Apps (and Users) Provided Consent (Count I).

Plaintiffs allege that Google intercepted their communications with apps in violation of section 2511(1)(a) of the federal Wiretap Act, 18 U.S.C. § 2510, *et seq*. Compl. ¶ 122. The essential elements of a section 2511(1)(a) claim are: (i) the intercepting, endeavoring to intercept, or procuring any other person to intercept a wire, oral, or electronic communication, and (ii) the doing of such acts intentionally. 18 U.S.C. § 2511(1)(a); *see also Backhaut v. Apple Inc.*, 148 F. Supp. 3d 844, 849 (N.D. Cal. 2015), *aff'd*, 723 F. App'x 405 (9th Cir. 2018).

The Wiretap Act provides that "[i]t shall not be unlawful...to intercept a wire, oral, or electronic communication . . . where one of the parties to the communication has given prior consent to such interception." *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1026 (quoting 18 U.S.C. § 2511(2)(d). "Since the Wiretap Act concerns the *unauthorized* interception of electronic communication, the consent of one party is a complete defense to a Wiretap Act claim." *Id.* (citing *Murray v. Fin. Visions, Inc.*, CV-07-2578-PHX-JM, 2008 WL 4850328, at *4 (D. Ariz. Nov. 7, 2008) (emphasis in original)).

The Wiretap Act claim fails because the apps (and users) provided consent. Plaintiffs allege that "[w]hen Google collects such information via Firebase, Google intercepts private communications between app users and the app publisher." Compl. ¶ 38. But, as explained above, the apps choose to use Firebase to collect their users' data and agree to Google's collection of that data. *Id*. ¶¶ 41–42. Accordingly, there can be no question that the use of Firebase is authorized by the apps and exempt under the Wiretap Act. *See In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1026 ("Since the Wiretap Act concerns the *unauthorized* interception of electronic communication, the consent of one party is a complete defense to a Wiretap Act claim.").

C. Plaintiffs Fail to State a Claim Under the California Invasion of Privacy Act ("CIPA") (Count II).

Plaintiffs allege that Google violated Sections 631 and 632 of the California Invasion of Privacy Act ("CIPA"). But Plaintiffs have failed to state a claim under either section. Both the

Section 631 and 632 claims fail because Plaintiffs consented to Google's collection of the collected data. And the Section 632 claim fails because Plaintiffs have not plausibly alleged an actionable privacy interest under these circumstances.

1. The Section 631 and 632 claims fail because Plaintiffs consented to Google's collection of the data.

"The California Supreme Court has held that Section 631 protects against three distinct types of harms: 'intentional wiretapping, willfully attempting to learn the contents or meaning of a communication in transit over a wire, and attempting to use or communicate information obtained as a result of engaging in either of the two previous activities.'" *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1036. Consent of the parties to the communication is a complete defense to a Section 631(a) claim. *See Matera v. Google Inc.*, No. 15-CV-04062-LHK, 2016 WL 5339806, at *7 (N.D. Cal. Sept. 23, 2016) ("Under CIPA, a consent defense is established when both parties—the sender and the recipient of the communication— consent to the alleged interception."); *see also In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 607 (citing Cal. Pen. Code § 631(a) ("CIPA prohibits any person from using electronic means to 'learn the contents or meaning' of any 'communication' 'without consent' or in an 'unauthorized manner.'")).

"Section 632 is part of California's invasion of privacy statutory scheme. It provides, in relevant part, that "'[e]very person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic ... device ... records the confidential communication' violates the statute." *Weiner v. ARS Nat. Servs., Inc.*, 887 F. Supp. 2d 1029, 1032 (S.D. Cal. 2012) (citing Cal. Pen. Code § 632(a)). "Accordingly, the three elements that Plaintiff must prove are (1) an electronic recording of (or eavesdropping on); (2) a 'confidential' communication; and (3) all parties did not consent." *Id.* (citing *Flanagan v. Flanagan*, 27 Cal. 4th 766, 774–76, 117 Cal. Rptr. 2d 574 (2002)).

Plaintiffs have failed to, and cannot, plead that all parties to the alleged communications (i.e. Plaintiffs and the apps) did not consent to Google's conduct. As explained supra § IV(A)(1)–(3), both the apps and Plaintiffs specifically consented to the collection of the underlying data. Plaintiffs'

Section 632 claim thus fails as a matter of law and should be dismissed. *See, e.g., Maghen v. Quicken Loans Inc.*, 94 F. Supp. 3d 1141, 1146 (C.D. Cal. 2015), *aff'd in part, dismissed in part*, 680 F. App'x 554 (9th Cir. 2017) (section 632 claim failed because the parties to communication consented to defendant's conduct).

2. Plaintiffs have not plausibly alleged that their interactions with apps were confidential under Section 632.

Plaintiffs' Section 632 claim also fails because they do not plausibly allege what information was collected and accordingly how they expected that the information was confidential. Under Section 632, "a conversation is confidential if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard." *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1051 (N.D. Cal. 2018) (citing *Flanagan*, 27 Cal. 4th at 766); *see also Flanagan* 27 Cal. 4th at 772–73 (adopting the confidentiality test set out in *Frio v. Superior Court*, 203 Cal. App. 3d 1480, 1488, 250 Cal, Rptr. 819 (1988)). This test is objective. *Id.* Plaintiffs' subjective expectation of privacy is therefore irrelevant to the inquiry. *Id.* at 766–77*; Coulter v. Bank of America Nat'l Tr. & Savings Ass'n*, 28 Cal. App. 4th 923, 929, 33 Cal. Rptr. 2d 766 (1994) ("the test of confidentiality is objective" and a party's subjective intent is irrelevant). In deciding whether a communication is confidential under Section 632, courts consider the surrounding circumstances to determine whether the parties had an objectively reasonable expectation that the conversation is not being recorded or overheard." *Faulkner v. ADT Sec. Servs., Inc.*, No. C 11-00968 JSW, 2011 WL 1812744, at *3 (N.D. Cal. May 12, 2011) (citing *Flanagan*, 27 Cal. 4th at 776–77 (collecting cases)).

Here, Plaintiffs have not plausibly alleged that the data they shared with the apps was objectively confidential. Rather, they imply that they did not expect Google to collect it because they decided to turn off WAA. *See, e.g.,* Compl. ¶¶ 71 ("Plaintiffs…had a reasonable expectation of privacy that when using non-Google branded apps while having opted out of 'Web & App Activity' tracking, Google would not intercept, collect, record, disclose, or otherwise misuse their personal communications and data."); *id.* at ¶ 121 ("[T]he communications intercepted by Google

were plainly confidential, which is evidenced by the fact that Plaintiffs turned off 'Web & App Activity."). Plaintiffs further allege that the content of the allegedly private communications were (i) the title of the page that they viewed in the apps, (ii) the "page_referrer (*i.e.*, if the user arrived at that page via another page), and (iii) the page URL. *Id*. ¶ 38. Plaintiffs allege that the communications contained "personal" and "private" information, but provide no factual allegations in support. *Id*. ¶ 59-60.

These allegations fail to state a Section 632 claim. Plaintiffs must allege that the information they shared with the apps is confidential and provide facts supporting those allegations. *See In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) ("Nor is the court required to accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." (citation and quotation marks omitted)). It is not enough to simply allege that they did not expect *Google* to collect the information. And it is unlikely that Plaintiffs could allege a confidential communication here. *See, e.g.*, *In re Google Assistant Privacy Litig.*, No. 19-cv-04286-BLF, 2020 WL 2219022, at *8 (N.D. Cal May 6, 2020) (citing *Sunbelt Rentals, Inc.*, 43 F. Supp. at 1035 (finding that certain electronic communications were not confidential within the meaning of Section 632); *see also Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) (same).

Plaintiffs barely plead what data may have been collected and only identify data showing the title of the app page they visited, whether they arrived at that page from another page, and the page URL. Compl. ¶ 38. They do not even allege that this information was personally attributable to Plaintiffs or that they included any personally identifiable information, perhaps because the Firebase ToS and Use Policy forbid apps from sharing users' personally identifiable information with Google. Rope Decl. ¶ 2 and Ex. 1(a)-(b), pp. 4, 14; *id.* ¶ 3 and Ex. 2(a)–(b), pp. 1, 3. Plaintiffs have failed to allege an objectively confidential communication.

D. Plaintiffs Fail to State a Claim for Invasion of Privacy Under the California Constitution (Count III).

To state a claim for invasion of privacy under the California Constitution, "Plaintiff must show that: (1) they possessed a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is 'so serious … as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F. 3d at 601 (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009)). Because of the similarity in the tests for common and Constitutional invasion of privacy claims, "courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *Id.* Plaintiffs fail to plausibly plead either of these elements.

1. Plaintiffs fail to allege an actionable privacy interest.

As discussed above, because Plaintiffs consented to Google receiving this data and because they have not sufficiently alleged that any of it is confidential, Plaintiffs have not plausibly plead that Google somehow violated their reasonable expectation of privacy. *First*, Plaintiffs consented to Google receiving the underlying data (as discussed supra § II(A)(1)–(3)), which obviates a reasonable expectation of privacy in that information. *See Smith v. Facebook, Inc*, 262 F. Supp. 3d 943, 955–56 (N.D. Cal. 2017); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1037-38 (holding that a plaintiff asserting a privacy claim under the California Constitution "must not have manifested by his or her conduct a voluntary consent" to defendant's conduct) (quoting *Hill*, 7 Cal. 4th at 26). *Second*, as explained above, Plaintiffs fail to plausibly allege that the information Google allegedly collected is objectively confidential. Plaintiffs have thus failed to allege information upon which an invasion of privacy claim can be based. *Cf. Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal 2012) (plaintiffs did not adequately state a claim for invasion of privacy where they did not allege that anyone "de-anonymize[d]" their "browsing history" data even if it could be de-anonymized).

2. Plaintiffs fail to allege a highly offensive invasion of privacy that constitutes an egregious breach of social norms.

The "California Constitution … set[s] a high bar for an intrusion to be actionable." *In re Google Assistant Privacy Litig.*, 2020 WL 2219022, at *19 (citation and quotation marks omitted). Plaintiffs have failed to plausibly allege that Google receiving users' basic app activity data constitutes a "highly offensive" invasion of privacy or "an egregious breach of social norms."

Here, the fact that apps authorized Google to collect data regarding anonymized users' activity within an app is hardly the type of "egregious breach of social norms" that could constitute a constitutional violation. Courts in this district have made clear that collection of the type of information at issue in this case is routine commercial behavior that does not give rise to a "highly offensive" invasion of privacy. *See, e.g., In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1050, 1063 (N.D. Cal. 2012) (citing *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal.App.4th 986, 992, 125 Cal.Rptr.3d 260 (2011)); *see also Moreno v. San Francisco Bay Area Rapid Transit Dist.*, No. 17-cv-02911-JSC, 2017 WL 6387764, at *8 (N.D. Cal. Dec. 14, 2017) (accessing anonymous data from an app, even when the app is not in use, would not be highly offensive or egregious to a reasonable user); *Yunker v. Pandora Media, Inc.*, No. 11-CV-03113 JSW, 2013 WL 1282980, at *15 (N.D. Cal. Mar. 26, 2013) (no actionable privacy violation where the Pandora app collected plaintiff's PII and provided that information to advertisers); *Low*, 900 F. Supp. 2d at 1015 (LinkedIn did not commit a "highly offensive" invasion of users' privacy by disclosing users' browsing histories to third parties); *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (Google's collection and disclosure of users' data, including their browsing histories, "do not plausibly rise to the level of intrusion necessary to establish an intrusion claim."); *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1063 ("[D]isclos[ure] to third parties [of] … unique device identifier number, personal data, and geolocation information from Plaintiffs' iDevices … does not constitute an egregious breach of social norms." (citation omitted)).[3]

[3] Indeed, the type of conduct that meets this element is a far cry from what is alleged here. *See Susan S. v. Israels*, 55 Cal. App. 4th 1290, 1298, 67 Cal. Rptr. 2d 42, 47 (1997) ("stranger's

E. Plaintiffs Fail to State a Claim Under CDAFA, Cal. Pen. Code § 502(c) (Count IV).

Plaintiffs fail to state a claim against Google for violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA") because: (a) Google was authorized to access Plaintiffs' app activity data, and (b) Plaintiffs have not alleged that Google circumvented any technical or code-based barriers to access the data.

1. Google was authorized to collect Plaintiffs' app activity data.

Plaintiffs cannot state a claim under section 502(c) of CDAFA where, as here, the defendant was authorized by the apps, not to mention the users themselves, to access and use the information at issue. *See Oracle USA, Inc.* 879 F.3d at 962 (holding that plaintiffs cannot state a claim under CDAFA where the defendant had authorization to take and use the information upon which the CDAFA claims is based); *see also Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 131–32 (N.D. Cal. 2020) (dismissing CDAFA claim because defendant had authorization to access plaintiffs' data).

2. Plaintiffs do not allege that Google accessed their data by circumventing any technical or code-based barriers.

CDAFA prohibits "knowingly accessing, and without permission, using any data, computer, computer systems, or computer network" in certain prohibited ways. Cal. Pen. Code § 502. To adequately plead that a party acted "without permission" under CDAFA, a plaintiff must allege that defendant "circumvent[ed] technical or code-based barriers in place" to prevent unauthorized access. *See Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1053 (N.D. Cal. 2018).

Moreover, Plaintiffs do not allege that Google accessed their app activity data by circumventing "technical or code-base barriers." Compl. ¶¶ 151-158. Instead, Plaintiffs merely allege that Google accessed their data in contravention of the WAA setting being off, "Plaintiffs had expressly communicated to Google that Google did not have permission to take, copy or make

---

unauthorized reading and dissemination of a person's mental health records is a serious invasion of the person's privacy."); *Givens v. Regents of Univ. of Cal.*, No. G030663, 2003 WL 21246766 (Cal. Ct. App. May 30, 2003) (disclosure of an employee's whistleblower status violated the employee's constitutional right of privacy).

use of such data." Compl. ¶152. But 502 addresses efforts to circumvent technical or code-based barriers, which are never alleged here. *See, e.g.*, *In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *10 (N.D. Cal. Sept. 20, 2011) (citing Cal. Pen. Code § 502); *see also In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 716 (N.D. Cal. 2011) ("It is thus impossible, on Plaintiffs' own allegations, for Defendant to be liable under the subsections of Section 502 which require a defendant to act 'without permission,' as there were clearly no technical barriers blocking Defendant from accessing its own website.").

Nor is it plausible that Google "circumvented" technical, code-based or any other barriers, because, as explained above, the apps authorized Google to collect the information *using Firebase*, a tool developers intentionally integrated into their apps for that very purpose. *See* Compl. ¶ 33 ("Google itself explains to app developers that "Firebase '[a]utomatically collected events are triggered by basic interactions with your app. As long as you use the Firebase SDK, you don't need to write any additional code to collect these events."). Thus, not only have Plaintiffs failed to allege that Google "circumvented" technical or code-based barriers in apps by using Firebase, it is implausible.

V. CONCLUSION

For these reasons, Google respectfully requests that the Court dismiss Plaintiffs' Complaint in its entirety with prejudice.

DATED: October 13, 2020

Respectfully submitted,

WILLKIE FARR & GALLAGHER LLP

By: /s/ *Benedict Y. Hur*

Benedict Y. Hur